Ser. No. 09/936,479
Customer No. 24498

REMARKS

This application has been reviewed in light of the Office Action dated June 19, 2007. Claims 1-4, 8 and 9 are pending in the application. By the present Amendment, claims 1 and 3 have been amended, and claims 8 and 9 have been added. No new matter is believed to be introduced. The Examiner's reconsideration of the rejection in view of the amendment and the following remarks is respectfully requested.

By the Office Action, claim 1 stands rejected under 35 U.S.C. §103(a) as being unpatentable over by U.S. Patent No. 5,351,294 to Matsumoto et al. (hereinafter Matsumoto) in view of U.S. Patent No. 5,103,479 to Takaragi et al. (hereinafter Takaragi).

Claim 1, as amended recites, *inter alia*, a method for managing access to a signal representative of an event of a service provider including ... (b) receiving, in said smart card, data representative of a first seed value, the first seed value representing a first point in a coordinate system; (c) generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, the second seed value representing a second point in the coordinate system, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card; and (d) descrambling, in said smart card, said signal using said generated scrambling key to provide a descrambled signal.

In accordance with claim 1, the first and second seed values are points in a coordinate system, and the scrambling key is generated by the smart card using the first and second seed values. Further, the first seed value is supplied by a service provider and the second seed value is permanently stored in the smart card. This approach permits more than one service provider to share the stored second seed value, and each service provider is free to choose its

own first seed value. The present claim elements and the flexibility provided thereby are not taught or suggested by the cited combination.

Matsumoto includes a **limited** broadcast system that sends data encrypted at an information service station 104 out to receiving stations. The information service station generates an encryption or cipher key K by using destination information I (see FIG. 2, bbck 202). The destination information I is sent to a receiving station which also employs the destination information and other information to generate the cipher key K (see FIG. 3, block 305) at the receiving station.

The limited broadcast system of Matsumoto must know which of the receiver stations are permitted to decrypt the encrypted data. The destination information (I) includes a string of 1's and 0's that indicate which receiver stations have permission to decrypt the data stream and which do not. This presupposes that each received station must be known by the information service provider 104 before a transmission is made. This is method is limited due at least to this limitation. While a secure system may be achieved by Matsumoto, the system does not provide the flexibility afforded by the method in accordance with the present invention.

In addition, Matsumoto does not disclose or suggest a second seed value permanently stored in the smart card. Instead, Matsumoto, provides a computed k value that is determined based upon a present time that is read when the encrypted data is received (see col. 6, lines 27-30). While the IC card of Matsumoto includes a hash function, the hash function is a sum check that computes the cipher key K based on the parameter k and the number of blocks of the destination information. This is a dynamic computation that is only based on the information

sent to the card. According to the present invention, a permanent second seed is not computed, but is instead stored permanently on the smart card.

Matsumoto fails to teach all of the elements of claim 1. In particular, Matsumoto fails to disclose or suggest at least receiving, in said smart card, data representative of a first seed value, the first seed value representing a first point in a coordinate system; generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, the second seed value representing a second point in the coordinate system, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card; and descrambling, in said smart card, said signal using said generated scrambling key to provide a descrambled signal.

The Examiner has cited Takaragi to cure the deficiencies of Matsumoto. However, Takaragi fails to cure these deficiencies. Takaragi is directed to an encipher/decipher method which employs a smart card to supply keys for a high speed computational method. The smart card (112) stores keys (e.g., K_1 to K_4) to be introduced to the encipher/decipher equipment 100.

At col. 16, lines 25-32, Takaragi describes that the smart card may include a microcontroller to substitute for the CPU 110 of equipment 100. The Examiner cites this portion of Takaragi to teach that scrambling operations may be performed on a smart card. While such processing may, *arguendo*, be performed on the smart card, Takaragi fails to teach or suggest at least: receiving, in said smart card, data representative of a first seed value, the first seed value representing a first point in a coordinate system; generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, the second

seed value representing a second point in the coordinate system, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card. In Takaragi, keys are stored only on the smart card, whether the smart card is only a card or includes a processor. Further, two different seed values obtained from different sources are not both used to determine an encryption key.

Neither Mutsumoto and/or Takaragi, taken singly or in combination, teach or suggest receiving, in said smart card, data representative of a first seed value, the first seed value representing a first point in a coordinate system; generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, the second seed value representing a second point in the coordinate system, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card. The cited combination fails to teach that the first and second seed values are part of a coordinate system and that the first seed value is received by the smart card while the second seed is permanently stored on the smart card. Therefore, claim 1 and claims 2-4 are believed to be in condition for allowance for at least the stated reasons. Reconsideration of the rejection is earnestly solicited.

By the Office Action, claim 1 stands rejected under 35 U.S.C. §103(a) as being unpatentable over by Matsumoto in view of Takaragi and further in view of U.S. Patent No. 6,760,445 to Schwenk et al. (hereinafter Schwenk).

The Examiner has cited Schwenk to teach a Euclidean plane in the context of an encryption system. However, Schwenk is directed to a system that tracks encryption keys distributed to users to determine who has betrayed the correct usage of the keys. A surface in space is defined along which users are assigned. All encryption keys that were distributed to a

given user must pass through a point in the surface for that user. If not, the user who leaked that key can be identified, since that key will indicate its assigned origin.

Schwenk fails to cure the deficiencies of Matsumoto and/or Takaragi. Therefore, claims 2-4 are believed to be in condition for allowance due at least to their dependency from claim 1. Other reasons exist for allowing claims 2-4. For example, Schwenk fails to teach or suggest at least that first and second seed values are points on a Euclidean plane and that a Y-intercept of a curve formed on said Euclidean plane is calculated by said first and second seed values. Schwenk is instead directed to a completely different operation and solve a completely different problem. Reconsideration of the rejection is earnestly solicited.

In view of the foregoing amendments and remarks, it is respectfully submitted that all the claims now pending in the application are in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Ser. No. 09/936,479
Customer No. 24498

PD990014

A Petition for an extension of time is enclosed. The Patent Office is authorized to charge the extension fee to Applicant's Attorney Deposit Account No. 07-0832. It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to applicant's Deposit Account No. 07-0832.

Respectfully submitted,

Dated: 12/6/07

By: _____
Paul Kiel
Registration No. 40,677
(609) 734-6815

Mailing Address:

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312